



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,358	01/14/2000	Ernst-Michael Hamann	GE-99-008	8276

7590

04/22/2004

James E Murray  
69 South Gate Drive  
Poughkeepsie, NY 12601

EXAMINER

KIM, JUNG W

ART UNIT PAPER NUMBER

2132

DATE MAILED: 04/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/483,358

Applicant(s)

HAMANN ET AL.

Examiner

Jung W Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 23 February 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 23 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

1. Claims 1-25 have been examined.

***Drawings***

2. The drawings were received on February 23, 2004. These drawings are acceptable.

***Response to Amendment***

3. The objection to the title of the invention has been withdrawn, as the revised title is more clearly indicative of the claimed invention.
4. The rejections under 112, first paragraph as listed in the previous office action have been withdrawn as the amended claims overcome the rejections.

***Claim Objections***

5. Claims 1-11, 15-17, 20, 21, 23, and 25 are objected to because each of these claims are not worded as a single sentence. Claim 22 is objected to because the first semicolon in the sentence should be a colon. Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1, 7, 8, and 19 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
8. Claims 1 and 19 recite the limitations "the certificate". There is insufficient antecedent basis for this limitation in the claims.
9. Claim 7 recites the limitation "the supplementary certificates". There is insufficient antecedent basis for this limitation in the claim.
10. Claim 8 recites the limitation "the individual keys and keys generated in step aa)". There is insufficient antecedent basis for this limitation in the claim.

***Claim Rejections - 35 USC § 103***

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over VeriSign 'Certification Practice Statement' version 1.2 (hereinafter VeriSign) in view of Sutter U.S. Patent No. 5,924,094 (hereinafter Sutter), Stallings Cryptography and Network Security 2<sup>nd</sup> Edition (hereinafter Stallings), and Karlton 'Proposal to add attribute certificates to TLS 3.1' (hereinafter Karlton). As per claim 1, VeriSign discloses a method of creating a certificate to certify a key (see VeriSign, 'Certification Practice

Statement', version 1.2), wherein the certificate comprises a defined number of data elements which at least contain information on the certification body (issuer of the certificate), the user of the certificate and the key certified by the certificate (see VeriSign, section 2.4.9, Figure 3). The method disclosed by VeriSign is characterized by the following steps:

- a. specification of a request for certification of one of several keys by a certification body for a user (see VeriSign, Section 4, 'Certification Application Procedures', especially section 4.2);
  - b. if in step a) only one key is to be certified, and no basic certificate is yet available for the user, creation of a basic certificate for the user with a defined number of data elements which, in the certification process, are identical for the respective user in conjunction with the respective certification body (see VeriSign, Section 4.2, under class 1 type: 'Method of Communicating Application');
  - c. addition of an identifying characteristic to the basic certificate (see VeriSign, section 2.4.9, Figure 3, serial number);
13. VeriSign is silent on the matter of certifying a plurality of keys in a single request. However, Sutter teaches the idea of a plurality of keys being certified as a single certificate, and hence as a single request (see Sutter, page 49, lines 35-39). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Sutter to the invention covered by VeriSign. Motivation for such a

Art Unit: 2132

combination would enable the plurality of keys to be used for different purposes by the subscriber to be assigned under one certificate as taught by Sutter.

14. Further, VeriSign does not explicitly disclose signing the certificate. However, Stallings teaches that signing messages is a conventional methodology to enable the receiver of the message to verify the origin of the message (see Stallings, page 300, first 3 bullets). More specifically, Stallings teaches that X.509 certificates are conventionally signed to verify that a certificate was generated by a trusted CA (see Stallings, page 342, Figure 11.3, especially signature data fields). It would be obvious to one of ordinary skill in the art at the time the invention was made for the CA to sign the prototype certificate. The motivation for such an implementation would enable the certificate applicant to verify the CA processing the request. Hence, the method disclosed by VeriSign in view of Stallings further includes the following steps:

- d. generation of a digital signature for the basic certificate and addition of the digital signature to the basic certificate (see Stallings, page 342, Figure 11.3, especially signature data fields);
- e. generation of a key pair: inherent in the inclusion of a public key data value in the certificate disclosed by VeriSign is the generation of a key pair - public and private keys (see VeriSign, section 2.4.9, Figure 3; see Stallings, page 342, Figure 11.3, subject's public-key info data field).

15. VeriSign is silent on the matter of a supplementary certificate. However, supplementary certificates have been a major topic among those skilled in the art as it has become well recognized that the X.509 v3 protocol does not meet many of the

Art Unit: 2132

certificate format requirements that new and emerging secure network transactions require. The X.509 v3 protocol attempted to deal with these concerns with extensions to the basic certificate format; however, these additions did not fully anticipate the growing diversity of network transactions. In light of these concerns, the notion of paired certificates began to establish itself among those skilled in the art: the combined use of an identity certificate (another name that describes the current X.509 certificate), which distinctly identifies the subject of the certificate, and an attribute certificate, which links the subject with one of a varied number of transaction types, would address the limitations of an X.509 v3 certificate. Karlton discloses an attribute certificate having similar syntax as an X.509 v3 certificate that further extends the use of the identity certificate (see Karlton, page 1, 'What are Attribute Certificates', 'Motivation'; page 2, paragraph 6). He discloses that the attribute certificate augments an identity certificate with additional attribute fields and is associated with the identity certificate by an identifier (see Karlton, page 2, paragraph 7). In addition, since an attribute certificate is a signed object that asserts additional properties of an identity certificate (see Karlton, page 1, 1<sup>st</sup> paragraph), the attribute certificate also includes a digital signature separate from the one of the basic certificate. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to create a supplementary, signed certificate to augment the basic certificate in the invention disclosed by VeriSign. The motivation for such a combination would enable a standard certificate to take on additional attributes as new traits are found to be desirable without persistently changing the structure of the standard certificate, as disclosed by Karlton (see Karlton,

page 1, 1<sup>st</sup> paragraph, 'Motivation'). Hence, the invention disclosed by VeriSign in view of Stallings and Karlton also includes the following steps:

- f. creation of a supplementary certificate for the basic certificate with a key as set out in step e), the identifying characteristic as set out in step c) and additional data fields not registered by the basic certificate (see Karlton, page 1, 1<sup>st</sup> paragraph; page 2, 'Implementation Outline');
- g. generation of a digital signature for the supplementary certificate and addition of the digital signature to the supplementary certificate (see Karlton, page 1, 1<sup>st</sup> paragraph).

16. Finally, although VeriSign is silent on the matter of using only one key when this one key shares redundant information with other existing and future basic certificates, this final step is a general economizing feature using relational organization. When there exists redundant information with respect to a certain thing, the redundant information is typically coalesced with the certain thing. For example in the related field of relational database schema design, identity tables are typically mapped as one-to-one correspondence with a subject set, each subject having a primary key id, whereas redundant information (attributes of each subject) is mapped to this identity table using foreign key ids, and these attributes corresponding to tables defining different types of attributes. Therefore, examiner takes Official Notice that coalescing redundant information is a notoriously well-know teaching and applies to the invention covered by Verisign. It would be obvious to one of ordinary skill in the art at the time the invention was made to use the basic certificate for keys that share redundant information.



Art Unit: 2132

Motivation for such a combination would enable economization of certificates and use a well-known relational organization to associate keys to a subscriber. The aforementioned covers claim 1.

17. As per claim 2, VeriSign covers a method of creating a certificate to certify a key outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the basic certificate comprises the following data elements: name of certification body, user id of certification body, name of user, user id of user, and identifying characteristic of the basic certificate (see Stallings, page 342, Figure 11.3 (a)).

18. As per claim 3, VeriSign covers a method of creating a certificate to certify a key outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the supplementary certificate comprises the following data elements: signature algorithm, validity period of the certificate, extensions, and an identifying characteristic of the basic certificate (see Karlton, page 2, 6<sup>th</sup>-7<sup>th</sup> paragraph; see Stallings page 342, Figure 11.3(a) and pages 347-349, 'X.509v3'). VeriSign is silent on the matter of a key and a key serial number being present in the supplementary certificate. However, with the emergence of different key usages (see Stallings, page 348, bullet 'Key Usage'), keys now establish a type of transaction, and as such, they do not solely identify a subject (since now a subject can have multiple keys). Therefore, it would be obvious to one of ordinary skill in the art to store the key data in the supplementary certificate. The motivation for such an implementation would enable the basic certificate to store

information only relevant to the subject and also support the notion of the supplementary certificate as maintaining information relevant to relationships between the subject and other entities (events, organizations, etc.). This motivation is commonly found in the related field of relational databases and can be applied to the public key infrastructure. Furthermore, VeriSign requires that all CAs under the VeriSign PKI retain records for all material events, including key generation, so that an audit trail can be established (see VeriSign, section 3.8 and 3.9). By including a serial number that identifies the key in the supplementary certificate, key identification would be retained (and hence the source of the key generation) within the certificate, and thus establish a convenient reference to the key's history. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the supplementary certificate to store the key serial number. The motivation for such an implementation would promote users trust in the certificate. The aforementioned covers claim 3.

19. As per claim 4, VeriSign covers a method of creating a certificate to certify a key outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Stallings discloses that extensions to the X.509 certificate have been incorporated in the third version to categorize key use of the public key in a certificate (see Stallings, page 348-349, 'Key usage', 'Certificate policies', and 'Policy mappings'). Among other reasons, these fields have been incorporated to distinguish the different types of keys for different transaction scenarios (see Stallings, page 348, requirement 5). Finally, as outlined above, Sutter teaches incorporating several keys into one certificate, and the step of eliminating

redundancies using a relational organization is a well-known and well-established means. Hence, the invention covered by VeriSign covers claim 4.

20. As per claim 5, VeriSign covers a method of creating a certificate to certify a key outlined above in the claim 4 rejection under 35 U.S.C. 103(a). In addition, the certificate contains the following data elements: name of certification body, user id of certification body, name of user, user id of user, type and version of the certificate, key, validity, serial number, and extensions (see Stallings, page 342, Figure 11.3). Furthermore, inherent in the combination case of obviousness disclosed in the claim 4 rejection, the certificate includes the number and types of keys as data fields.

21. As per claim 6, VeriSign covers a method of creating a certificate to certify a key outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the steps of the method disclosed by VeriSign in the event that no basic certificate exists cover the steps defined in claim 6 in the event when a basic certificate already exists. Hence, claim 6 is rejected under VeriSign in view of Sutter, Stallings, and Karlton for the same reasons set forth in the rejection of claim 1.

22. As per claim 7, VeriSign covers a method of creating a certificate to certify a key outlined above in the claim 3 and 6 rejections under 35 U.S.C. 103(a). In addition, the supplementary certificates each contain the following data elements: signature algorithm, key, serial number of key, validity period of the certificate, extensions, and

identifying characteristic of the basic certificate (see Karlton, page 2, 6<sup>th</sup>-7<sup>th</sup> paragraphs; see Stallings page 342, Figure 11.3(a) and pages 347-349, 'X.509 v3').

23. As per claims 8-11, they are method claims corresponding to claims 1-7 and they do not teach or define above the information claimed in claims 1-7. Therefore, claims 8-11 are rejected under VeriSign in view of Sutter, Stallings, and Karlton for the same reasons set forth in the rejections of claims 1-7.

24. As per claim 12, VeriSign covers a method for creating a certificate for the simultaneous certification of several keys as outlined above in the claim 8 rejection under 35 U.S.C. 103(a). In addition, the key is a public key (see Stallings, page 342, Figure 11.3(a), subjects public-key info).

25. Claims 13-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over VeriSign in view of Sutter, Stallings, and Karlton, and further in view of Deo et al. U.S. Patent No. 5,721,781 (hereinafter Deo). As per claims 13 and 14, VeriSign covers a method of creating a certificate to certify a key outlined above in the claim 4 rejection under 35 U.S.C. 103(a). Although VeriSign is silent on the matter of storing the generated certificates in the non-volatile memory of a smart card, it is conventional in the art for key data to be stored in secured portable devices. For example, Deo discloses an authentication system where certificates are stored in the ROM of a smart card (see Deo, col. 12, lines 7-22; Figure 2). It would be obvious to one of ordinary skill

in the art at the time the invention was made to store the generated certificates in the non-volatile memory of a smart card. Motivation for such a combination would enable the user to mate the benefits of smart card portability and processing capability without compromising the privacy of the key data as disclosed by Deo (see Deo, col. 1, line 55-67).

26. As per claims 15 and 16, VeriSign covers a method of creating a certificate to certify a key outlined above in the claim 14 rejection under 35 U.S.C. 103(a). In addition, Deo discloses that the certificate is stored/loaded into the RAM of a smart card (see Deo, col. 12, lines 7-22; Figure 2). Hence, the aforementioned covers both claims 15 and 16.

27. As per claims 17 and 18, they are method claims corresponding to claims 14, 15, and 16 and they do not teach or define above the information claimed in claims 14, 15, and 16. Therefore, claims 17 and 18 are rejected under VeriSign in view of Sutter, Stallings, and Karlton, and further in view of Deo for the same reasons set forth in the rejections of claims 14, 15, and 16.

28. Claims 19-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over VeriSign in view of Sutter, Stallings, and Karlton as applied to claims 1-7 and further in view of JAVA 'X.509 Certificates and Certificate Revocation Lists' (hereinafter JavaAPI). As per claims 19-25, VeriSign covers a method for creating a certificate to certify a key

as outlined above in the claim 1-7 rejections under 35 U.S.C. 103(a). VeriSign is silent on the matter of the method being incorporated into a computer program product on a computer usable medium. JavaAPI discloses a certificate API that can be used to access and manage certificates (see JavaAPI, page 4, java.security.cert package). It would be obvious to one of ordinary skill in the art at the time the invention was made to implement the methods disclosed by VeriSign into a computer program product using the Java API offered by SUN Microsystems. Motivation for such a combination would enable the method disclosed by VeriSign to be implemented into a marketable product. The aforementioned covers claims 19-25.

### ***Response to Arguments***

29. Applicant's arguments filed February 23, 2004 have been fully considered but they are not persuasive. In response to applicant's argument that the references teach away from incorporating a key pair in the attribute certificate as taught by Karlton (see applicant's arguments, page 21, 1<sup>st</sup> paragraph), the examiner points out that this particular teaching by Karlton is a means to distinguish and define attribute certificates relative to an identity certificate and the relationship established between attribute and identity certificates. The obvious construction formed in the rejections by the examiner using Karlton is not a construction between an identity certificate and an attribute certificate but a combination between a basic certificate covered by the invention of VeriSign, Sutter, and Stallings, and a modified attribute certificate (supplemental certificate as named in the applicant's claim); as such, this teaching by Karlton does not

Art Unit: 2132

establish a nonobviousness rebuttal. Furthermore, since, the content of certificates are merely digital means of structuring information between users, key values, and other pertinent information, any invention based on the way certificates are organized fails to meet the patentability requirement of an inventive step when it is based on well principled design criteria as is the case in the invention claimed by the applicant. Hence, the amended claims are rejected over the prior art of record.

### ***Conclusion***

30. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

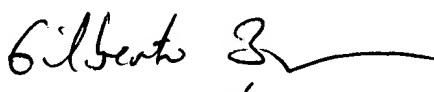
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung W Kim  
Examiner  
Art Unit 2132

Jk  
April 8, 2004



GILBERTO BARRÓN  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100